

# E-Mail and Internet Safety



**City of Seattle**

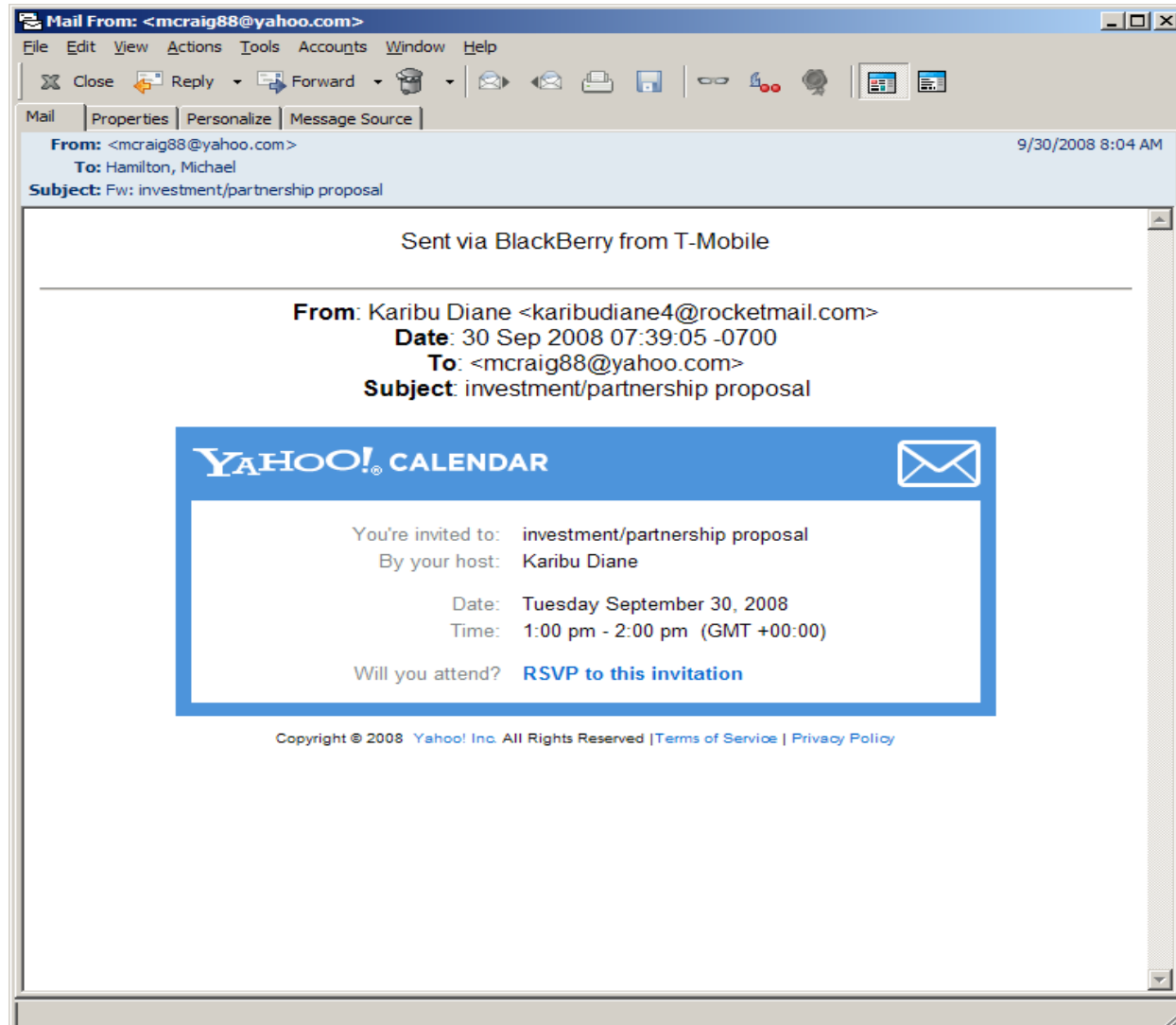
**Office of Information Security**

# E-MAIL ATTACKS

- You have received a card from an admirer!
- Nigerian 419, or Advance-Fee scams
- Become an EBay Powerseller!
- Your card was used in Bulgaria
- You've won the European e-mail lottery!
- Saddam Hussein Found Alive!
- Japan Tsunami video
- Unreadable Twitter messages
- Your Facebook password has been reset
- National Intelligence Council report



# 419 MEETING INVITATION!



# Pump-n-Dump

- Carnegie Cooke & Company, Inc. (CGKY)  
A Huge PR campaign is expected starting Wednesday and all next week so grab as much as you can up to \$0.25 range.
- Infinex Ventures Inc. (IFNX) = OTC: IFNX.OB  
This One is Strong UP 0.50 (28.57%) Jan 9th Alone  
Huge PR Campaign Running for Tuesday Jan 10th  
We expect explosive growth thru Friday



# FAKE FACEBOOK MESSAGE

## Facebook Password Reset Confirmation! Your Support.

Facebook Security [customer@facebook.com]

Sent: Tue 3/23/2010 7:30 AM

To: Boone, Kathy (SCL)

Message | Facebook\_password\_139.zip (41 KB)

Dear user of facebook,

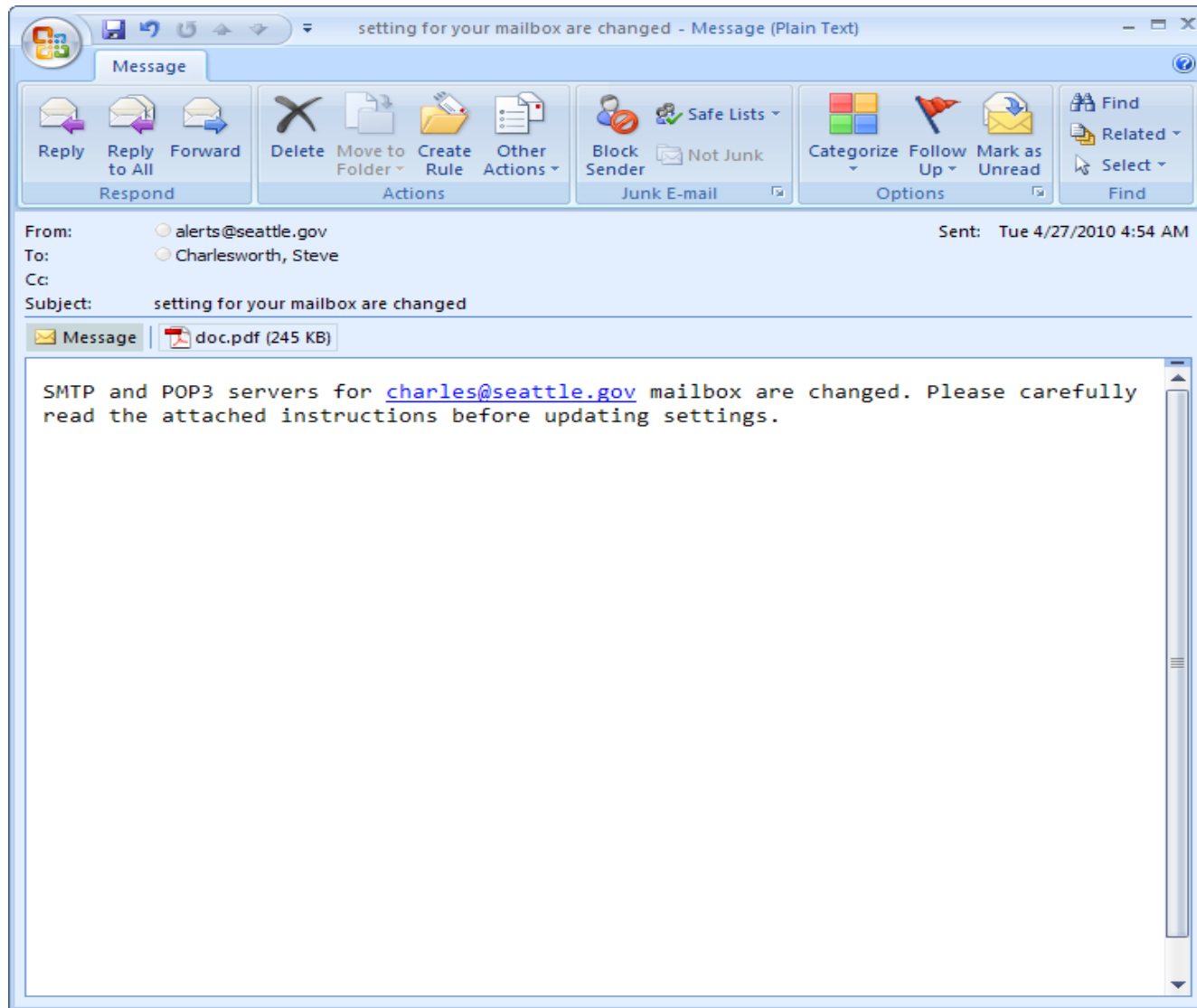
Because of the measures taken to provide safety to our clients, your password has been changed.  
You can find your new password in attached document.

Thanks,  
Your Facebook.



All folders are up to date. Connected to Microsoft Exchange

# FAKE SUPPORT MESSAGE



# WHAT WAS WRONG WITH THOSE?

- Your real name was not used in the e-mail
- Grammar and spelling errors
- There is no European e-mail lottery
- You didn't expect any of these
- You're logged into Facebook right now, and know perfectly well they haven't reset your password!



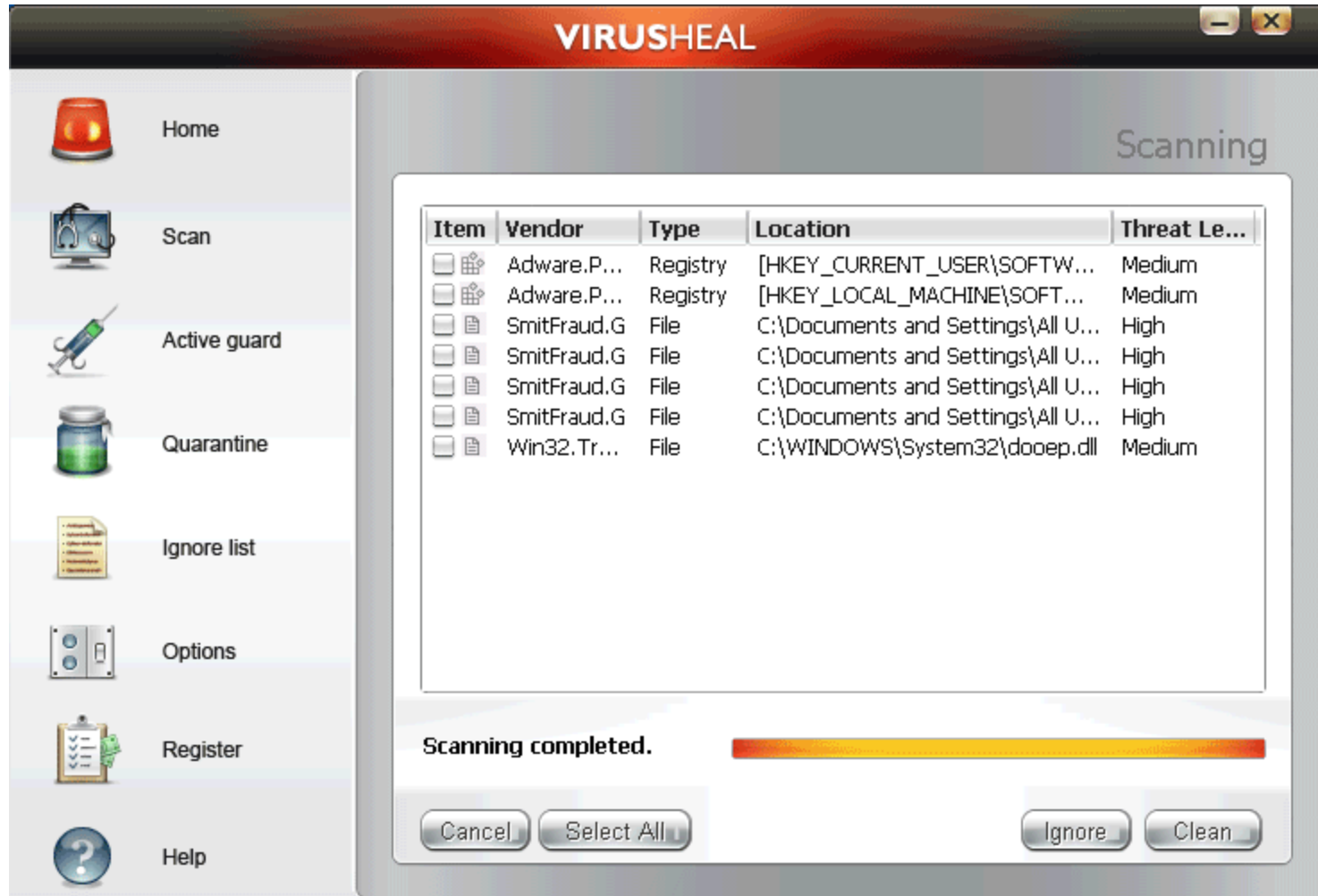
# HOSTILE WEBSITES

- Can exploit vulnerabilities on your computer just by visiting – “drive-by downloads”
- Usually deploy adware and spyware
- Golf site, gambling site – it doesn't matter
- Russian (and other) kits available to equip websites with deployment functionality: \$999.00
- 285,000,000 clicks to compromised sites every month
- Newer payloads are keystroke loggers, botnet downloaders, etc





# DRIVE-BY DOWNLOAD



# WEBSITE BOOBY-TRAP KITS

[Статистика](#)[Зараженные](#)[Рефералы](#)[Управление](#)

## Загрузка файла [?]

 [Browse...](#) [Загрузить](#)

(Текущий файл: 33792 байт)

## Выполнить действие

☐ Очистка статистики[Выполнить](#)

## Смена пароля

Новый логин

Новый пароль

[Сменить](#)

# WHAT MAKES THESE WORK?

- Bad decisions on the part of the user
- Vulnerable computers
- Readily-available exploits
- Use of psychology on the part of the threat actors, e.g. P2P and social networking bait



# Questions ?



***David R Matthews***

***david.matthews@seattle.gov***

***City of Seattle***

***Office of Information Security***